Humboldt-Universität zu Berlin
Institut für Informatik

Selbstdatenschutz

Unterrichtsentwurf

Inhaltsverzeichnis

1 Unterrichtsvoraussetzungen

1.1 Vorstellung der Unterrichtseinheit

Die Schüler/innen als Teil der Informationsgesellschaft müssen über ihr Recht auf die freie Entfaltung ihrer Persönlichkeit aufgeklärt werden. Die damit einhergehenden Probleme sind zu berücksichtigen: Durch die ständige Ausweitung der elektronischen Datenverarbeitung besteht die Möglichkeit, Querbezüge zwischen den unterschiedlichsten Informationen herzustellen. Somit kommt es zu einem Informationsnetz mit einem umfassenden Bild unserer Person und unserer Gewohnheiten. Wie diese Daten genutzt werden, ist dann fraglich. Dieser Sachverhalt wird als Teil des Berliner Rahmenlehrplans für die Oberstufe gefordert. Die Probleme des Datenschutzes und der Datensicherheit sollen erkannt werden. Notwendig ist eine Abgrenzung der Begriffe: Der Datenschutz bezeichnet den Schutz personenbezogener Daten vor Missbrauch. Er steht für die Rechte einzelner Personen an ihren Daten. Jeder soll grundsätzlich frei entscheiden, wem, wann, welche seiner persönlichen Daten zugänglich gemacht werden, also die informationelle Selbstbestimmung. Die Verhinderung des gläsernen Menschen in der Zukunft. Die Datensicherheit soll für den Schutz wichtiger Daten sorgen. Ziel ist die Verhinderung durch Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen. Der Schutz muss durch technische und organisatorische Maßnahmen gewährleistet werden, denn nur wenn die Daten wirklich sicher sind, werden auch die Rechte jedes Einzelnen geschützt. Durch Selbstdatenschutz und die Kenntnisse über Datenschutz und Datensicherheit soll den Schüler/innen alle Möglichkeiten an die Hand gegeben werden, um sich selbst um den Schutz der Privatsphäre zu kümmern. Dies ist Ziel der Unterrichtseinheit.

1.2 Stellung der Unterrichtssequenz

Die Unterrichtssequenz *„Selbstdatenschutz am Beispiel von verschlüsseltem Email-Verkehr“* ist Bestandteil der Unterrichtseinheit *„Selbstdatenschutz, Kenntnisse zum Datenschutz und zur Datensicherheit“* eines Informatik-Profilkurses der elften Jahrgangsstufe. In sieben Einzel- und in einer Doppelstunde werden folgende Themenbereiche abgehandelt.

- Problembewusstsein
- Rechtsgrundlagen
- Schützenswerte Daten
- Social networking
- Google
- Phishing und Pharming
- Selbstdatenschutz am Beispiel von verschlüsseltem Email-Verkehr
- Firewall

Die Unterrichtssequenz *„Selbstdatenschutz am Beispiel von verschlüsseltem Email-Verkehr“* erfolgt in einer Doppelstunde und knüpft an die Stunde zu „*Phishing und Pharming*“ an. Zentrale Punkte in der Unterrichtsequenz sind Kenntnisse über fehlende Datensicherheit bei der Nutzung des Internets und die Möglichkeit des Selbstdatenschutzes beim Email-Verkehr durch *GnuPG (Gnu Privacy Guard)*.

2 Unterrichtsentwurf

2.1 Sachanalyse

2.1.01 Sniffer

Ein Sniffer ist eine Software zur LAN-Analyse, welches die Möglichkeit bietet, Datenverkehr eines Netzwerks zu empfangen, aufzuzeichnen, darzustellen und gegebenenfalls auszuwerten.[1]

Um an die Daten (z.B. der Emailverkehr von Absender zu Empfänger (Abbildung 1)) zu gelangen, kontaktiert der Capture Driver eines Sniffers die entsprechende Netzwerkkarte und gelangt somit an die Informationen, die die Netzwerkarte erreichen. Die Daten werden bis zur Analyse durch einen Filter, welcher Pakete (z.B. TCP auf Port 80) selektieren kann, zwischengespeichert.

[1] http://de.wikipedia.org/wiki/Sniffer (31.07.2007).

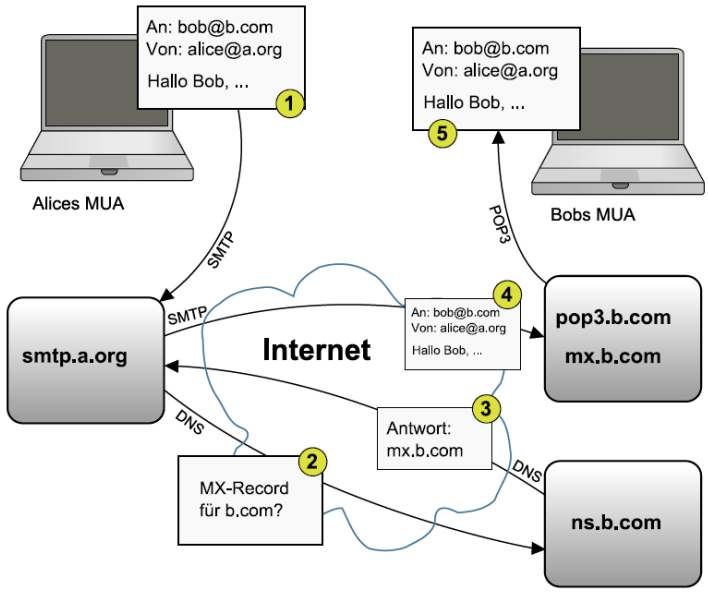

Abbildung 1: Email-Verkehr vom Absender zum Empfänger.
http://upload.wikimedia.org/wikipedia/commons/7/72/Wie_E-Mail_funktioniert.svg (31.07.2007).

Je nach Typ des Sniffers erfolgt die Analyse in unterschiedlichen Modi, man unterscheidet zwischen dem *non-promiscuous mode*, dem *promiscuous mode* und dem *monitor mode*. Im *non-promiscuous mode* werden die ankommenden und abgehenden Daten des eigenen Computers aufgezeichnet, im *promiscuous mode* wird der gesamte Datenverkehr im Netzwerk dokumentiert. Beide Modi sind bei LAN-Sniffern, der *promiscuous mode* bei aktiven WLAN-Sniffern zu finden. Der *monitor mode*, welcher bei passiven WLAN-Sniffern zum Einsatz kommt, sammelt nicht nur den Datenverkehr des Netzwerkes („Accesspoints“), sondern den gesamten Datenverkehr. [2] Eine Schutzmaßnahme bietet beispielsweise ein VPN-Tunnel. [3]

2.1.02 Rechtliche Aspekte des Abhörens von drahtlosen Verbindungen

Laut § 89 TKG sowie in § 202a StGB gibt es gesetzliche Regelungen, dass das Ausspähen von Daten bei der Kommunikation über drahtlose Netze nicht gestattet ist. Der § 89 TKG beschreibt das Abhörverbot von Nachrichten mit einer Funkanlage. Es ist festgelegt, dass das bewusste, also das vorsätzliche Abhören von Funkverbindungen verboten ist. Bei unbeabsichtigtem Abhören von ungesicherteren drahtlosen

[2] http://www.easy-network.de/sniffer.html (31.07.2007).
[3] Ahlers, Ernst: Spionageabwehr, 2007.

Verbindungen liegt laut § 89 Satz 1 TKG kein Verstoß vor. Bei unabsichtlichem Empfang dürfen weder der Inhalt der Nachrichten noch die Tatsache des Empfangs entsprechend § 89 Satz 2 TKG anderen nicht mitgeteilt werden. Das vorsätzliche Abhören, als auch die unbefugte Weitergabe sind nach § 148 Abs. 1 Nr. 1 TKG mit Strafe bedroht. Nur die vollendete Tat ist strafbar, nicht aber der Versuch.

Die unbefugte Beschaffung von Daten, welche gegen unberechtigten Zugang besonders gesichert und nicht für den Täter bestimmt sind, ist nach § 202a StGB strafbar. Diese Zugangssicherung soll den Zugang zu den Originaldaten, den Inhalten verhindern. Das Speichern von verschlüsselten Daten ist - aufgrund der fehlenden Möglichkeit auf die Originaldaten zuzugreifen - nicht strafbar. Durch eine Entschlüsselung der Daten erfolgt die Strafbarkeit. Nach § 205 StGB ist eine Strafverfolgung erst auf Antrag des Verletzten möglich. [4]

2.1.03 Merkmale für eine sichere Kommunikation

Um eine sichere Kommunikation via Email zu gewährleisten, sind drei Faktoren zu beachten: Authentizität, Integrität und Vertraulichkeit.
Unter Authentizität versteht man die überprüfbare Echtheit und Glaubwürdigkeit eines Subjektes oder Objektes. Sie dient als Grundlage für weitere Sicherungseigenschaften wie Integrität oder Vertraulichkeit. [5] Beim Email-Verkehr bedeutet die Authentizität die Zuordnung einer Email zum richtigen Absender, denn dieser kann leicht über SMTP gefälscht werden. Eine Absicherung ist durch eine digitale Signatur, wie sie *GnuPG* anbietet, möglich. [6]
Die Integrität charakterisiert den Schutz vor unautorisierter und unbemerkter Manipulation von Daten durch Personen. Daten dürfen nur durch Personen geändert werden, die die dafür nötigen Rechte besitzen.[7] Im Fall des unverschlüsselten Email-Verkehrs besteht die Gefahr, dass die Nachricht auf dem Weg verändert wird. Auch hier kann durch den Einsatz einer digitalen Signatur die Verlässlichkeit gewahrt werden. [8]

[4] http://www.datenschutz-bayern.de/technik/orient/oh_wlan.html#a1 (31.07.2007).
[5] http://wwwbayer.in.tum.de/lehre/SS2002/HSEM-bayer/Ausarbeitung1.pdf (31.07.2007).
[6] http://www.secure-it.nrw.de/_media/pdf/RZ_Sichere%20e-mail_150dpi.pdf (31.07.2007).
[7] http://wwwbayer.in.tum.de/lehre/SS2002/HSEM-bayer/Ausarbeitung1.pdf (31.07.2007).
[8] http://www.secure-it.nrw.de/_media/pdf/RZ_Sichere%20e-mail_150dpi.pdf (31.07.2007).

Die Vertraulichkeit beschreibt den Schutz vor unautorisierter Informationsgewinnung. Ziel ist es, dass Informationen nur jenen Personen zur Verfügung stehen, die die dafür nötigen Rechte besitzen. Über Zugangsrestriktionen wird meistens die Vertraulichkeit gewährleistet.[9] Im Fall des unverschlüsselten Email-Verkehrs erfolgt ein Transport im Klartext, welcher an vielen Stellen angezapft werden kann. Somit besteht eine unzureichende Zugriffsicherung, welche über Verschlüsselungstechniken verhindert werden kann. GnuPG bietet über symmetrische kryptographische Verfahren die Möglichkeit auf Vertraulichkeit.[10]

2.1.04 GnuPG

GnuPG ist unter der *GNU General Public License* stehende Kryptografie-Software auf Kommandozeilenebene. Die freie Software implementiert den OPENPGP-Standard entsprechend RFC2440 und erlaubt die Verschlüsselung und Signierung von Daten und Kommunikation.[11]

Für die Datenverschlüsselung wird das symmetrische kryptographische Verfahren *AES*, für das Schlüsselmanagement bzw. zur Signaturbildung asymmetrische kryptographische Verfahren wie *ElGamal*, *RSA* und *DSA/DSS* eingesetzt. *GnuPG* erstellt und verwendet asymmetrische Schlüsselpaare, einen privaten Schlüssel und genau einen zugeordneten öffentlichen Schlüssel. Der öffentliche Schlüssel (Abbildung 2) kann veröffentlicht werden, denn er dient dazu, die Nachrichten an den Besitzer des privaten Schlüssels zu verschlüsseln. Die mit dem öffentlichen Schüssel verschlüsselten Nachrichten können nur mit dem entsprechenden privaten Schlüssel (Abbildlung 3) entschlüsselt werden. Jene Nachrichten, die mit dem privaten Schlüssel signiert wurden, können nur mit dem öffentlichen Schlüssel des Absenders authentifiziert werden. Somit können die Integrität und die Authentizität gewahrt werden, denn *GnuPG* erstellt mittels des privaten Schlüssels des Absenders einen Prüfcode über die Nachricht, die digitale Signatur. Durch einen Abgleich mit dem öffentlichen Schlüssel kann festgestellt werden, ob der am Ende der Nachricht stehende Prüfcode übereinstimmt und die Nachricht unverändert ist. Um ein Höchstmaß an Schutz zu bieten, sollten Nachrichten oder Dateien standardmäßig mit dem privaten Schlüssel des Absenders signiert und anschließend mit dem öffentlichen Schlüssel des Emp-

[9] http://wwwbayer.in.tum.de/lehre/SS2002/HSEM-bayer/Ausarbeitung1.pdf (31.07.2007).
[10] http://www.secure-it.nrw.de/_media/pdf/RZ_Sichere%20e-mail_150dpi.pdf (31.07.2007).
[11] http://www.gnupg.org/(de)/features.html (31.07.2007).

fängers verschlüsselt werden. Die Umsetzung dieser beiden Funktionalitäten erfolgt in der Regel getrennt, verläuft aber für den Benutzer meist transparent.

Abbildung 2: Verschlüsselung. http://www.immerda.ch/index.php/Bild:Verschluesselung.png

Abbildung 3: Entschlüsselung. http://www.immerda.ch/index.php/Bild:Entschluesselung.png

Die Generierung des Schlüsselpaares erfolgt unter *GnuPG* von jedem Benutzer selbst. Dabei stehen unterschiedliche Einstellungsmöglichkeiten, wie beispielsweise die Schlüssellänge oder das Ablaufdatum des Schlüssels, zur Verfügung. Der private Schlüssel wird mittels Passphrase, auch Mantra genannt, vor unbefugtem Zugriff geschützt.

Bei der Nutzung des öffentlichen Schlüssels muss der Anwender sich davon überzeugen, dass dieser Schlüssel wirklich zu der angegebenen Person gehört. Dies kann über Zertifikate erfolgen, welche von vertrauenswürdigen Dritten vergeben werden. *GnuPG* bietet dem Nutzer die Möglichkeit, den öffentlichen Schlüssel anderer Personen mit Zertifikaten zu beglaubigen. Dies sollte jedoch nur dann erfolgen, wenn die Identität gesichert ist. Als Alternative kann über den sogenannten *Fingerprint*, einem Hashwert des öffentlichen Schlüssels, die Authentizität überprüft werden. Im Internet gibt es neben den Zertifizierungsstellen sogenannte Keyserver. Diese neh-

men Schlüssel in Empfang und verteilen die ungeprüften Schlüsselanfrage weiter. Eine Verifizierung der Authentizität kann über Fingerprints erfolgen.[12]

2.2 Didaktische Reduktion

Zum Beginn der Stunde werden die Schüler bezüglich ihres Wissens zum Email-Verkehr befragt, genauer, ob die Übermittlung vertraulich vonstatten geht. Nach Sammlung der Vermutungen werden zwei Schüler gebeten, sich von verschiedenen Rechnern Emails zu schreiben und diese anschließend zu beantworten.
Durch den Lehrer erfolgt die Präsentation der mittels Sniffer „abgefangenen" Pakete via Beamer. Dabei werden die Vermutungen der Schüler aufgegriffen und verdeutlicht, dass der Email-Verkehr nicht vertraulich erfolgt und die Daten im Klartext übermittelt werden. Die Funktionsweise von Sniffern und der Weg einer Email vom Absender zum Empfänger werden im Unterrichtsgespräch besprochen. Durch die weite Verbereitung von drahtlosen Verbindungen und den Möglichkeiten mit einfachen technischen Mittel diese abzuhören, müssen die rechtlichen Aspekte thematisiert und ein Rechtsbewusstsein geschaffen werden. Im Anschluss sollen die Schüler überlegen, welche weiteren Szenarien sie kennen, bei denen sie der Gefahr der „unfreiwilligen" Informationspreisgabe ausgesetzt sein könnten. Von den Beispielen ausgehend wird die gesamte Problematik (z.B. Passwortmissbrauch) einer „ungeschützten" Nutzung des Internets oder eines lokalen Netzes thematisiert, um den Schüler/innen Umfang der Gefahrenquellen zu zeigen.
Um eine theoretische Grundlage für eine sichere Kommunikation via Email zu schaffen und den Fokus auf eine Handlungsorientierung zu richten, sollen die Schüler/innen in Partnerarbeit die Merkmale einer sicheren Kommunikation beim Email-Verkehr im Internet recherchieren und diese dokumentieren. Eine Ergebnissicherung erfolgt bei der Besprechung des Arbeitsauftrags im Plenum. Etwaige Erfahrungen der Schüler/innen mit Schutzmöglichkeiten werden im Unterrichtsgespräch besprochen. Mittels der Beispielsoftware *GnuPG* wird eine Umsetzung von Authentizität, Integrität und Vertraulichkeit beim Email-Verkehr vom Lehrer vorgeführt. Nach einem Beispiel zur Sicherung von Authentizität und Integrität durch die digitale Signatur und einem Beispiel zur Wahrung der Vertraulichkeit durch Verschlüsselung, erarbeiten die Schüler/innnen die Thematik. Die Bearbeitung erfolgt wiederum in Partnerarbeit, um die

[12] http://www.bsi.de/gshb/deutsch/m/m05063.htm (31.07.2007).

soziale Eingebundenheit zu stärken, die Ergebnisse werden im Plenum besprochen und zur Ergebnissicherung am Whiteboard festgehalten. Der Vorgang der Konfiguration von *GnuPG* und somit das Rüstzeug für den Selbstdatenschutz, wird im Unterrichtsgespräch besprochen. Dabei werden die Erstellung eines Schlüsselpaares und die Veröffentlichung auf einem Keyserver demonstriert. Zum Abschluss der Stunde wird an deren Beginn angeknüpft, indem die Schüler diesmal verschlüsselte Mails verschicken. Die aufgezeichneten Nachrichten werden begutachtet und so die Erkenntnis gewonnen, dass die Nachrichten nun nicht mehr von Jedem einsehbar sind. Um die erlernten Inhalte auszuprobieren, sollen die Schüler/innen als Hausaufgabe *GnuPG* wahlweise graphisch oder kommandozeilenbasiert auf Ihrem Heimrechner installieren, konfigurieren und zum Abschluss eine Email an den Lehrer schicken.

2.3 Lernziele

- Wissensziele:
    - Die Schüler/innen sollen:
        - die Funktionsweise eines Sniffers beschreiben können,
        - die Begriffe Authentizität, Integrität und Vertraulichkeit definieren und in deren Rolle beim sicheren Email-Verkehr benennen können
        - rechtliche Aspekte des Abhörens von drahtlosen Verbindungen nennen können,
        - die Begriffe Digitale Signatur und Verschlüsselung mit privatem und offentlichen Schlüssel erklären,
        - das Prinzip der Verschlüsselungssoftware *GnuPG* erklären können.
- Könnensziele:
    - Die Schüler/innen sollen:
        - die Ver- und Entschlüsselung einer Email schematisch zeichnen können.
- Erziehungsziele:
    - Die Schüler/innen sind in der Lage:
        - konzentriert an den Computern zu arbeiten,
        - mit einem Partner zusammen zu arbeiten,

- die Gefahren einer unverschlüsselten Internetnutzung einschätzen zu können,
- die Bedeutung der Sicherheit bei Kommunikation per E-Mail zu kennen.

3 Weg- und Medienentscheidung

3.1 Methode

Der Schwerpunkt der Doppelstunde liegt im Wechselspiel zwischen Lehrervortrag, Unterrichts-Gespräch und Partnerarbeit. Dies ist notwendig, um die Inhalte der Vorführungsphasen mit den theoretischen Grundlagen zu verbinden. Das selbständige Erarbeiten der Inhalte steht im Vordergrund und schafft eine stärkere Auseinandersetzung mit der Thematik. Nach dem selbstständigen Erarbeiten werden die Inhalte im Unterrichtsgespräch gesammelt, eventuell korrigiert und zusammengefasst.

3.2 Medien

Die im Unterricht verwendeten Medien werden folgend aufgelistet. Die Mediennennung erfolgt einmalig, der jeweilige Einsatz wird beschrieben.

1. Whiteboard / Tafel:
    a. Das Whiteboard wird genutzt, um die Merkmale für einen sicheren Email-Verkehr anzuschreiben.
    b. Die schematische Darstellung des verschlüsselten Email-Verkehrs wird angezeichnet.
    c. Die Ergebnisse der Aufgabenstellung zur digitalen Signatur und zur Verschlüsselung werden am Whiteboard zusammengefasst.
2. Computer:
    a. Seitens der Schüler wird der Computer für das Schreiben der Emails und für die Recherche im Internet genutzt.
3. Beamer:
    a. Die Ergebnisse der Sniffers *Wireshark* und der Weg der Email vom Absender zum Empfänger werden mittels Beamer präsentiert.
    b. Die Vorführung von *GnuPG* erfolgt über Beamer.

4 Verlaufsplanung

Zeit [min]	Stoffgliederung	Didakt. Funkt. / Methoden	Lehrer	Schüler	Medien
09 min	Begrüßung		Ausblick zum Inhalt der Stunde		
	Einstieg	UG, EA	L. bittet SuS Vermutungen zu äußern, ob ihr Austausch von Emails vertraulich vonstatten geht?	SuS äußern ihre Vermutungen.	Rechner, Beamer
			L. bittet SuS Vermutungen zu äußern, ob ihr Austausch von Emails vertraulich vonstatten geht?	Zwei SuS schreiben sich mit zwei Test-Accounts abwechselnd unverschlüsselte Emails.	
			L. zeichnet Netzverkehr mittels Sniffer auf.		
			L. präsentiert die aufgezeichneten Daten, speziell der Email-Inhalt.	SuS sehen, dass die Email im Klartext zum Empfänger übertragen wird.	
12 min	Funktionsweise Sniffer	Lehrer-Vortrag, UG	L. erläutert die Funktionsweise eines Sniffers und den Weg einer Email zum Empfänger. Die rechtlichen Aspekte des Abhörens von drahtlosen Verbindungen werden vermittelt.	Aufnehmen und begreifen der Informationen.	
			L. bittet SuS weitere Szenarien zu nennen, bei denen Gefahren der Datenunsicherheit auftauchen können.	SuS nennen Gefahrenbereiche: jegliche unverschlüsselte Datenübermittlung	
			Verallgemeinerung der Datenunsicherheit auf jegliche unverschlüsselte Prozesse der Datenübermittlung. Hinführung zum Thema Selbstdatenschutz. Problemstellung: Fast jeder könnte meine Email lesen. Wie sieht aber eine sichere Kommunikation aus?		
10 min	Merkmale einer sicheren Kommunikation	AA, EA	L gibt Arbeitsauftrag: Merkmale einer sicheren Kommunikation beim Email-Verkehr sammeln und definieren.	SuS sammeln Merkmale einer sicheren Kommunikation beim Email-Verkehr und definieren diese.	Rechner, Internet
06 min	Besprechung der Merkmale einer	UG	Besprechung des Arbeitsauftrages: Vertrau-	SuS nennen und vergleichen ihre Ergebnis-	Whiteboard

	sicheren Kommunikation		lichkeit, Authentizität und Integrität. Zusammenfassung und eventuelle Ergänzung der Ergebnisse.	se.	
04 min	Möglichkeiten des Schutzes		L. bittet SuS Möglichkeiten des Schutzes zu nennen. Hinführung Selbstdatenschutz durch GnuPG.	PGP, HTTPS, VPN, etc.	
20 min	Transfer von Vertraulichkeit, Authentizität und Integrität auf GnuPG		L. führt das Signieren und Verschlüsseln von Emails beispielhaft vor. L. bittet die SuS die Unterschiede herauszuarbeiten und den Ablauf des verschlüsselten Email-Verkehres schematisch darzustellen.	SuS erarbeiten die Grundlagen zu Signierung und Verschlüsselung.	Rechner, Internet
13 min	Besprechung der Grundlagen zu Signierung und Verschlüsselung		Besprechung des Arbeitsauftrages. Zusammenfassung und eventuelle Ergänzung der Ergebnisse.	SuS erklären Digitale Signatur und Verschlüsselung durch öffentlichen und privaten Schlüssel. SuS skizieren Schema des verschlüsselten Email-Verkehres.	Whiteboard
09 min	Konfiguration von GnuPG für den Email-Verkehr.		L. demonstriert die Erstellung eines Schlüsselpaares und die Veröffentlichung auf einem Keyserver.	Aufnehmen und begreifen der Informationen.	Rechner, Beamer
05 min	Sniffen der Verschlüsselten Emails		L. zeichnet Netzverkehr mittels Sniffer auf und präsentiert den verschlüsselten Text!	Zwei SuS schreiben sich mit zwei Test-Accounts abwechselnd verschlüsselte Emails. SuS erkennen, dass die Nachricht verschlüsselt übertragen wird und nicht von jedem einsehbar ist.	Rechner, Beamer
02 min	Hausaufgabe	AA	L. bittet die SuS GnuPG wahlweise graphisch oder kommandozeilenbasiert auf Ihrem Heimrechner zu installieren, zu konfigurieren und eine Email an den Lehrer zu schicken.	SuS notieren die HA.	

5 Quellen

Zeitschriftenartikel:

Ahlers, Ernst: Spionageabwehr. Selbstschutz beim Surfen an WLAN-Hotspots. In: c´t, 2007,14, S. 204-207.

URL:

Widera, Sabine / Verweyen, Philip: Sicherheit für Informationssysteme. Begriffsbildung, Angriffsszenarien, *13.04.*2002.
Internet: http://wwwbayer.in.tum.de/lehre/SS2002/HSEM-bayer/Ausarbeitung1.pdf [31.07.2007].

Asmuth, Markus: secure-it in NRW. IT-Sicherheit macht Schule. Arbeitsmaterialien für den Unterricht. Sichere E-Mail-Kommunikation, 2005.
Internet: http://www.secure-it.nrw.de/_media/pdf/RZ_Sichere%20e-mail_150dpi.pdf [31.07.2007].

Bundesamt für Sicherheit in der Informationstechnik: Einsatz von GnuPG oder PGP.
Internet: http://www.bsi.de/gshb/deutsch/m/m05063.htm [31.07.2007].

Der Bayerische Landesbeauftragte für den Datenschutz: Orientierungshilfe: Datenschutz in drahtlosen Netzen, 2005.
Internet: http://www.datenschutz-bayern.de/technik/orient/oh_wlan.html#a1 [31.07.2007].

Stobitzer, Christian: *Sniffer, 19.09.*2006.
Internet: http://www.easy-network.de/sniffer.html [31.07.2007].

Wikipedia, Die freie Enzyklopädie: *Sniffer,* 27.07.2007.
Internet: http://de.wikipedia.org/wiki/Sniffer [31.07.2007].

GnuPG-Team: Features. Internet: http://www.gnupg.org/(de)/features.html [31.07.2007].